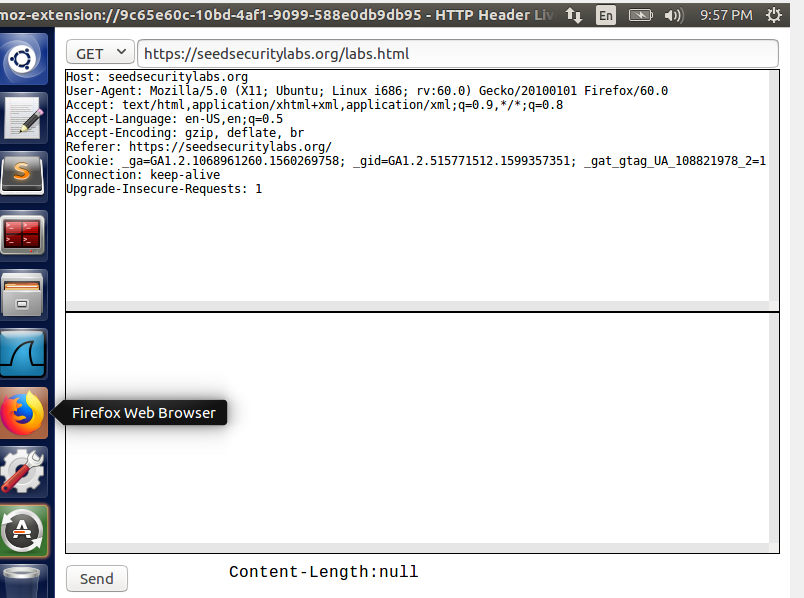
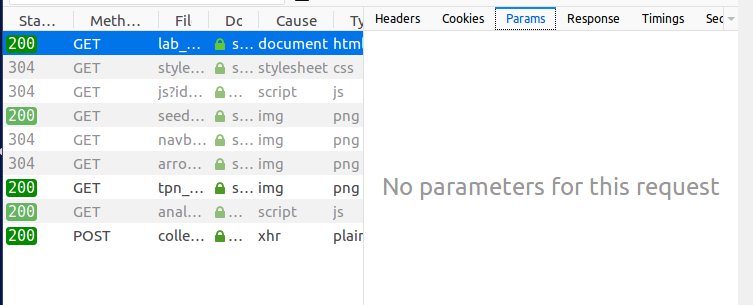
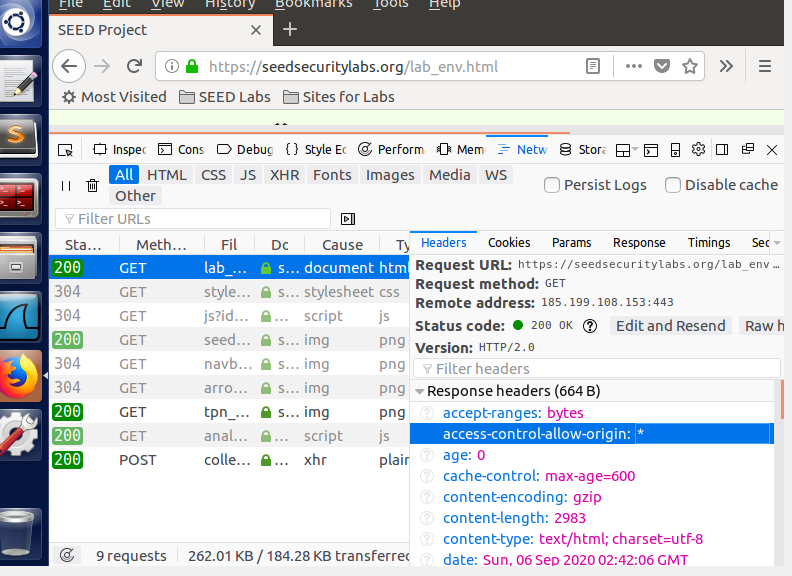
Cross-Site Request Forgery (CSRF) Attack Lab

(Web Application: Elgg)

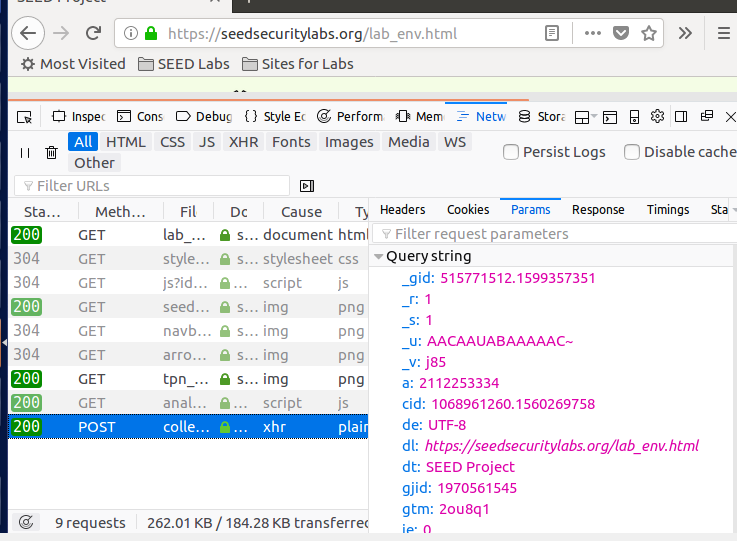
57118138 李嘉怡

**Task 1: Observing HTTP Request**

捕获HTTP GET请求：

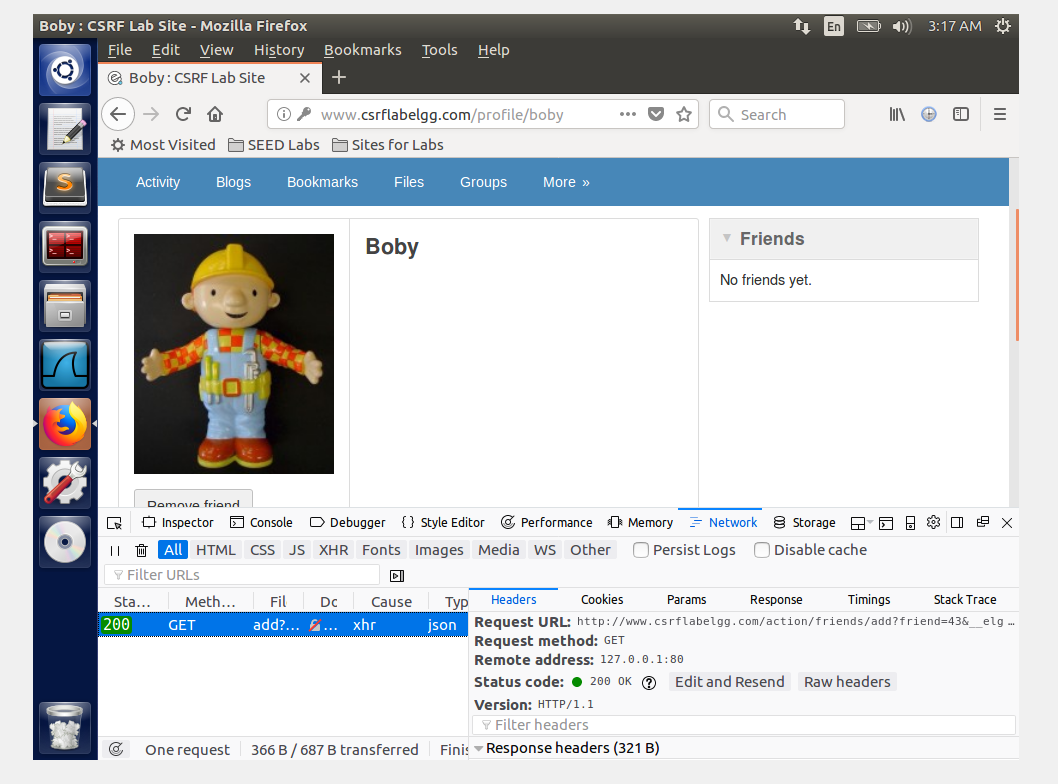


HTTP POST请求及参数：



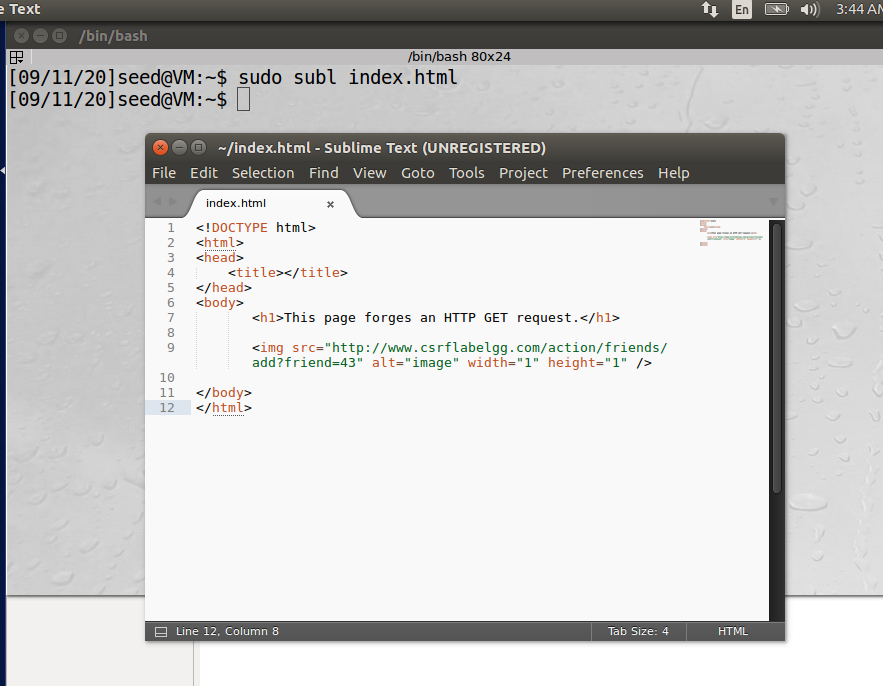
**Task 2: CSRF Attack using GET Request**

1. 首先，以Alice身份登录，搜索boby的信息，点Add Friends，从http GET的header中找到添加boby为好友的request URL：http://www.csrflabelgg.com/action/friends/add?friend=43&\_\_elgg\_ts=1599808569&\_\_elgg\_token=Vvm63pD。（之后要remove friend，以免影响后面测试）

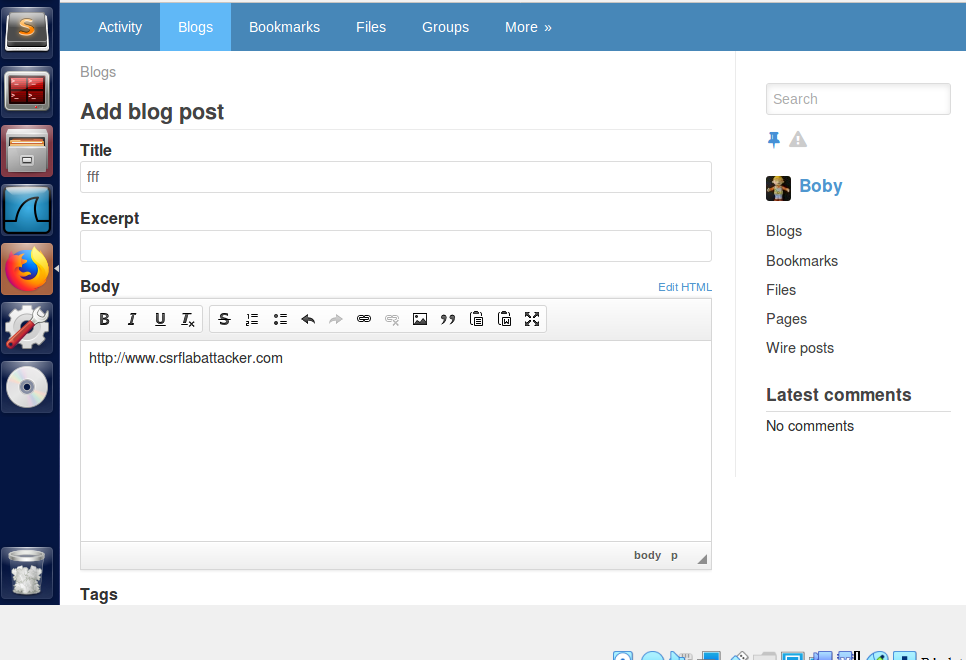


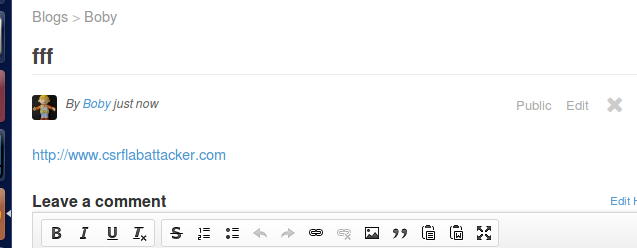
2.打开index.html，写入类似以下格式的代码创建网页，但是网址需要换成上一步找到的添加boby为好友的request URL。img标记将触发一个HTTP GET请求。当浏览器呈现一个web页面并看到一个img标记时，它会向src属性中指定的URL发送一个HTTP GET请求。攻击者使用add-friend URL和friend参数。图像的大小非常小，使受害者没有可疑。之后将这个网页放置在恶意网站www.csrflabattacker.com(在/var/ www/csrf/attacker文件夹内)。



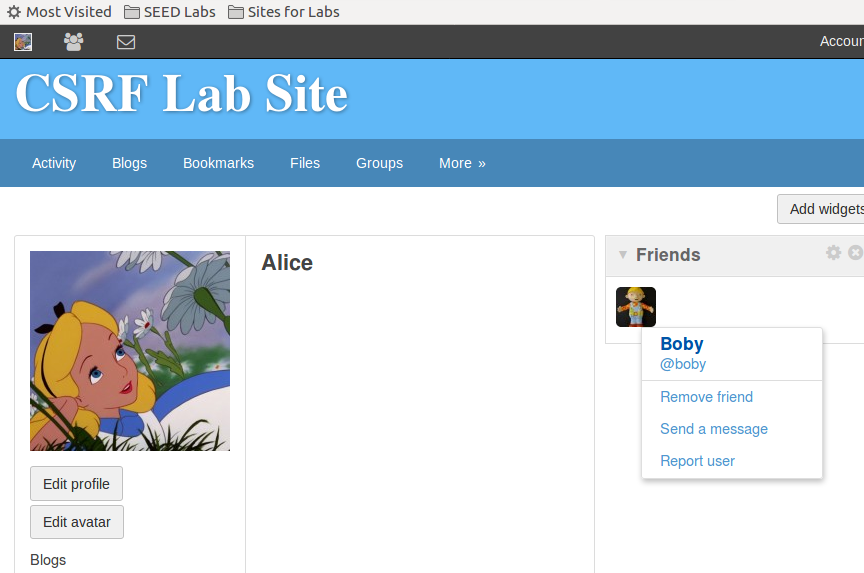
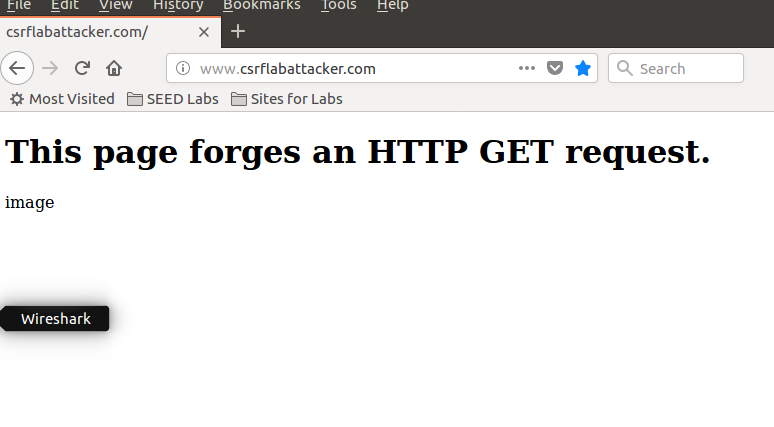
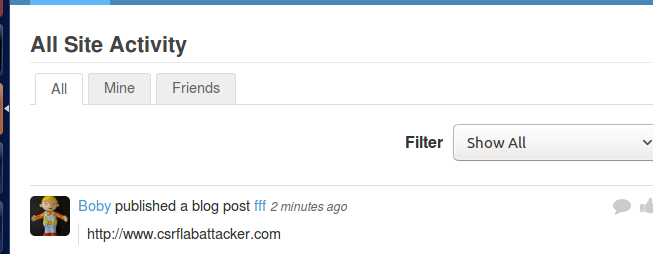


3.登入boby的账号，向Alice发送blog，里面包含攻击网站http://www.csrflabattacker.com。



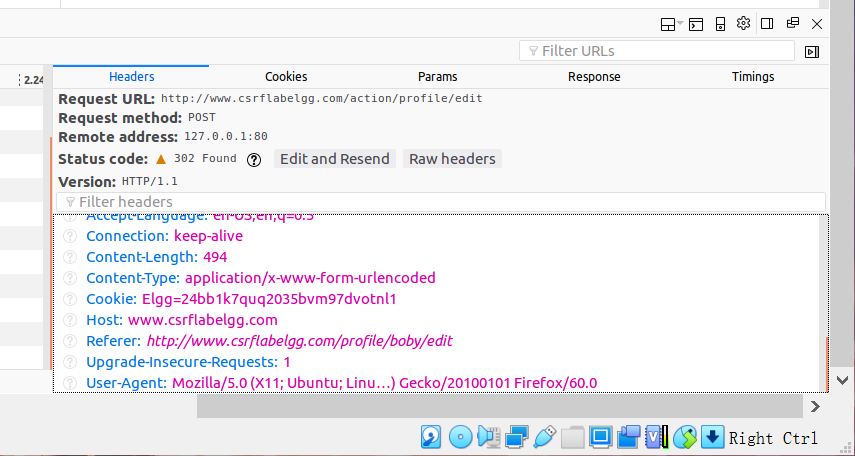
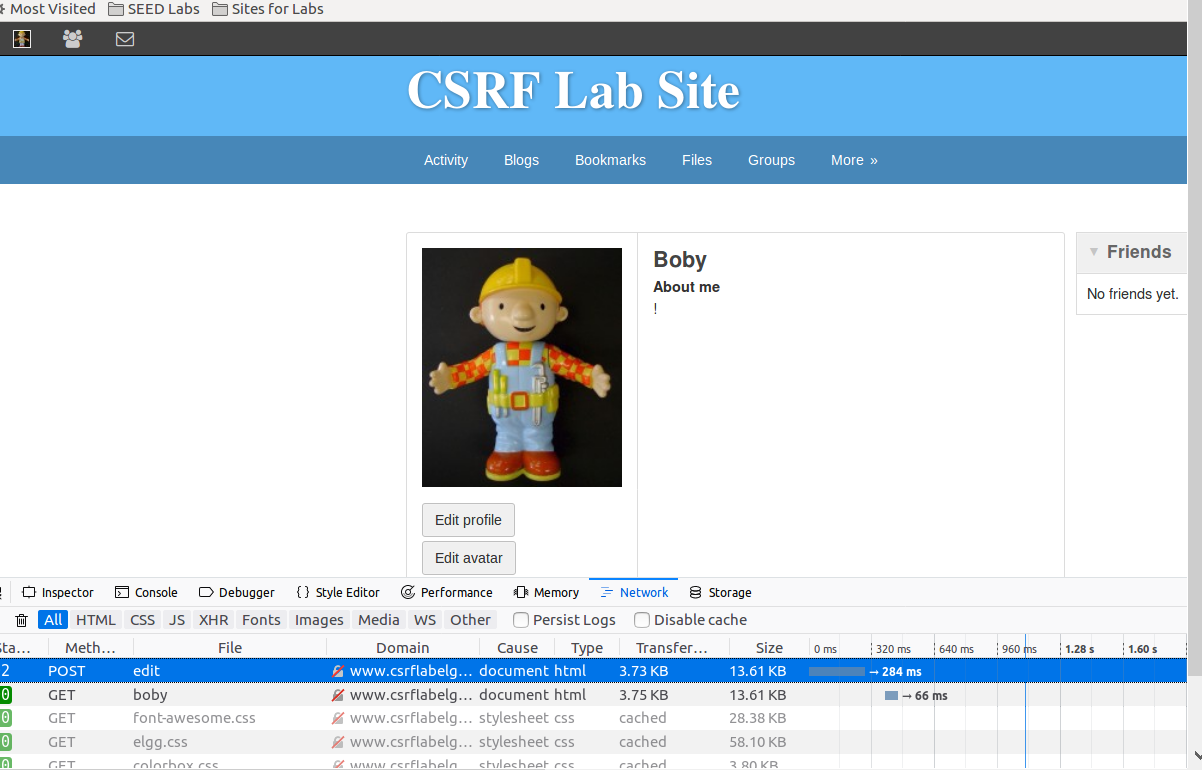


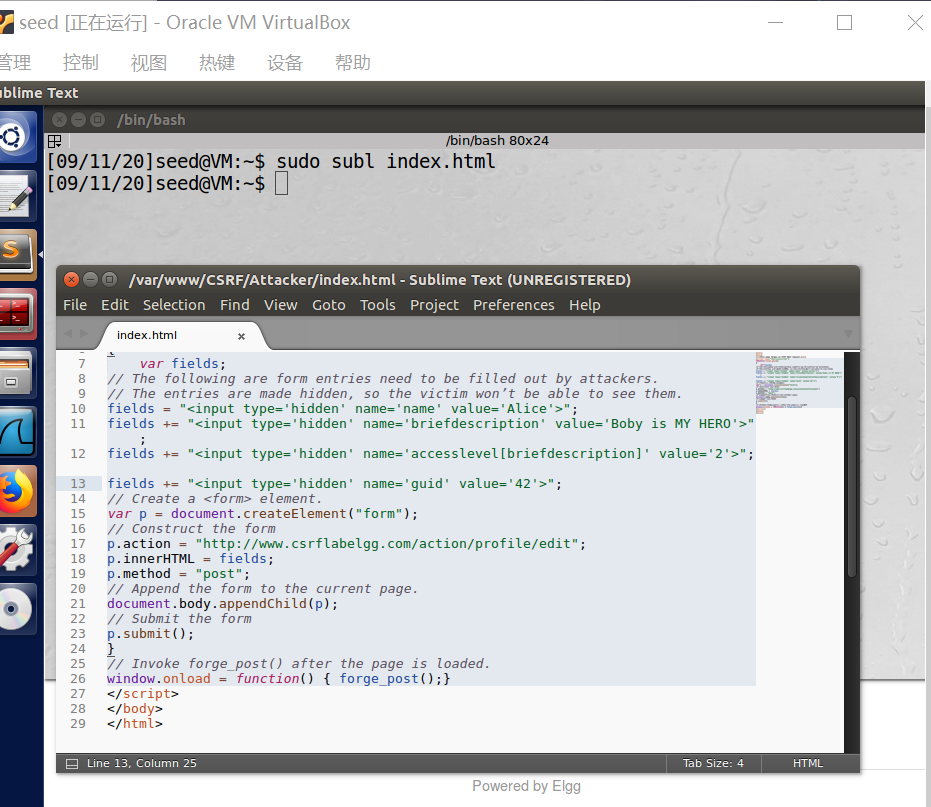
1. 登录Alice的账号。Alice收到boby发出的网址，出于好奇，当Alice访问web页面时，Boby就被添加到Alice的朋友列表中。

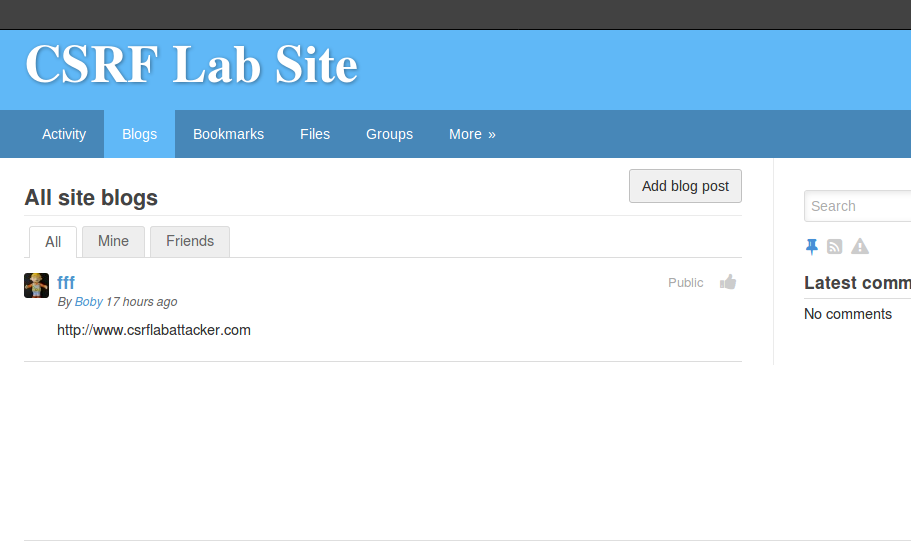


**Task 3: CSRF Attack using POST Request**

1. 登入boby的账号，edit profile，捕获post request，使得能够用其中提供的网址http://www.csrflabelgg.com/action/profile/edit来制作恶意网页。当受害者访问此页面时，表单将自动从受害者的浏览器提交(发布请求)“http://www.csrflabelgg.com/action/profile/edit”的编辑配置文件服务，导致该消息被添加到受害者的配置文件中。



1. 打开终端，打开index.html，将里面上一个实验的web代码修改为像下面格式的代码，其中包含上一步找到的网址http://www.csrflabelgg.com/action/profile/edit。
2. 登录Alice的账号,再次点击之前boby发送的网址，发现页面变成了新编辑过的样子。随后页面立刻跳转到Alice的profile界面，出现了Brief description：Boby is MY HERO。

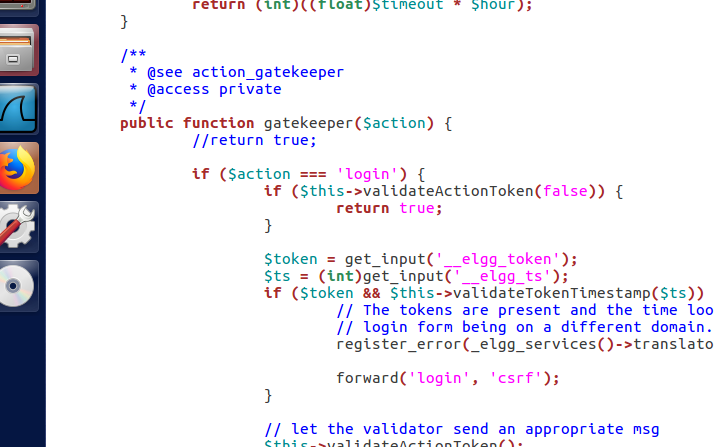


问题1：Boby可以先通过Alice之前的访问记录制造一个CRSF攻击，这个攻击的目的是获取Alice的guid，获取到以后再发动此次CSRF攻击。

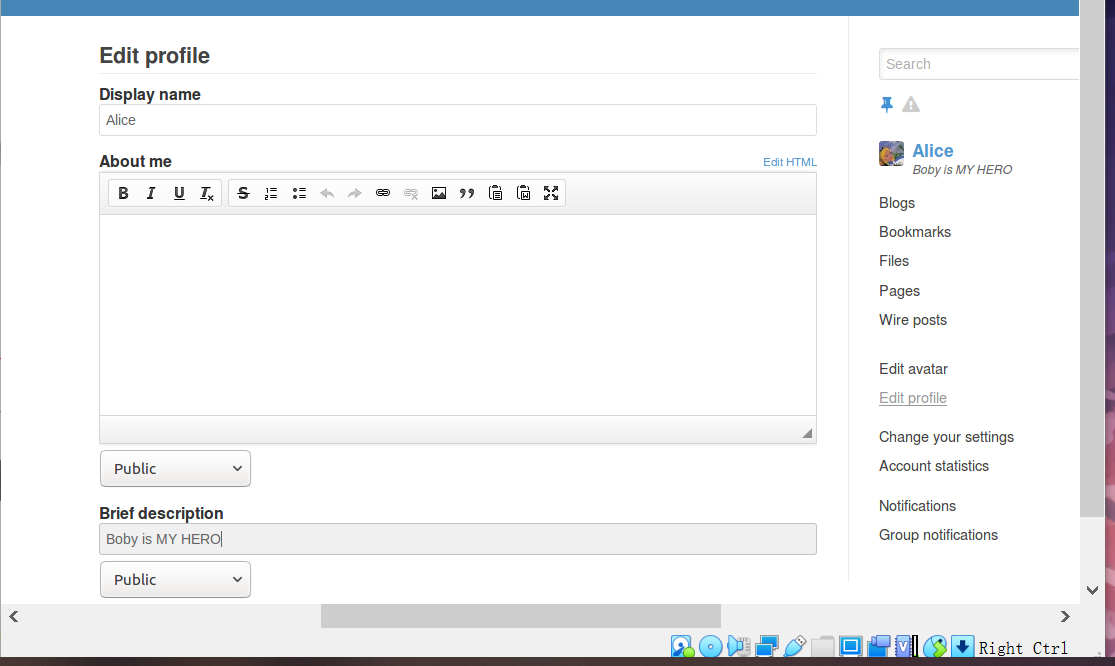
问题2：由于用户访问浏览器时会留下自己的cookie，攻击者可以攻击浏览器获得cookie，得到当前访问者的参数信息，然后用这些参数发动攻击。

**Task 4: Implementing a countermeasure for Elgg**

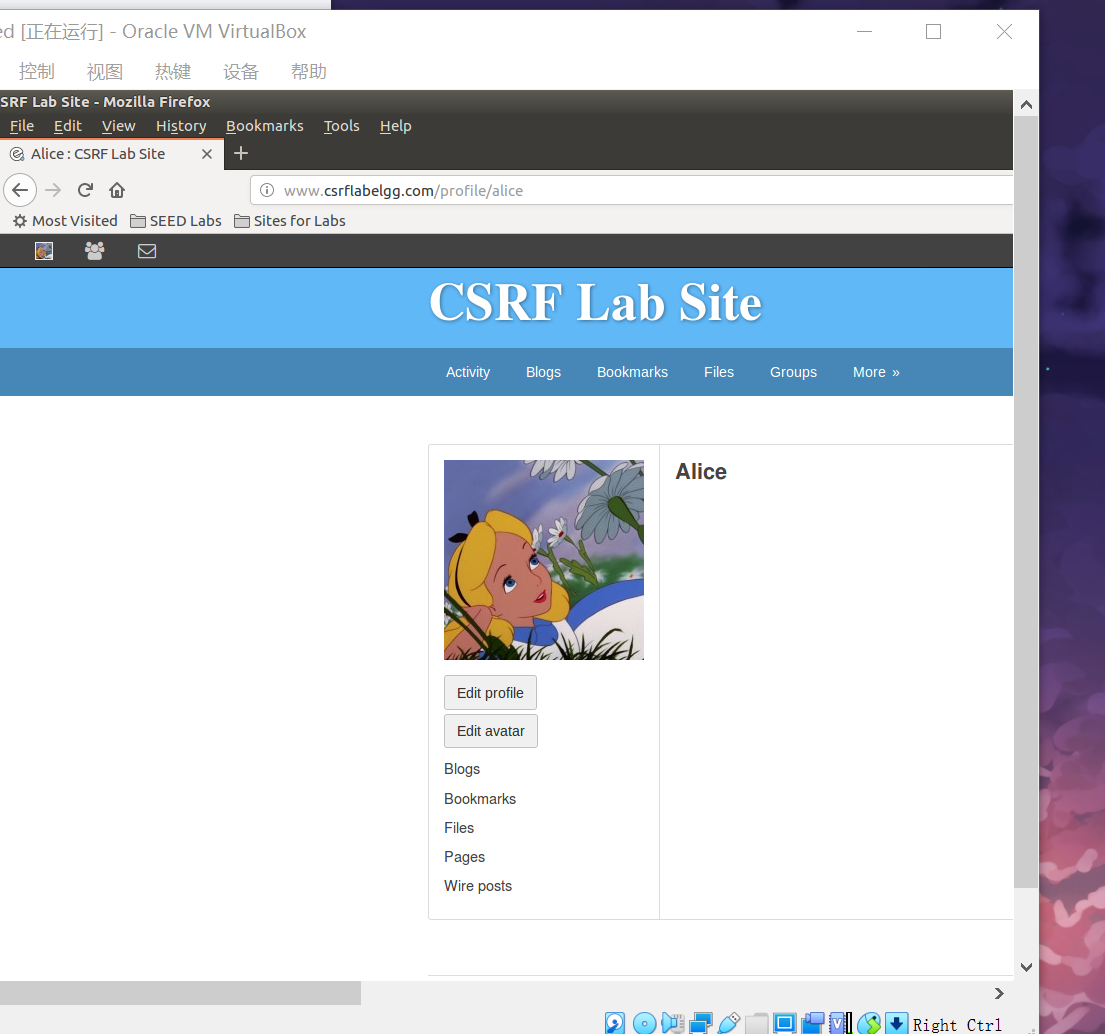
1. 在files中按下面路径找到文件ActionService.php，找到函数gateKeeper()，注释掉第一行的return true，使这句话下面的代码能够执行。



1. 在Alice账号中先把task 3添加的“Boby is'MY HERO”删除，以免对后续结果造成影响。



1. 再次点击Boby发来的网址链接，发现Alice的信息没有被修改。



原因是因为注释掉return true后，原来无法执行的代码得以执行，让程序验证生成的令牌和时间戳，每个用户操作都调用验证操作令牌函数，该函数验证令牌。如果令牌不存在或无效，操作将被拒绝，用户将被重定向，以抵御CSRF攻击。